Bilgi Dünyası 2006, 7(1): 121-146

Sayısal İmza ve Elektronik Belge Yönetimi

Digital Signature and Electronic Document Management

Kemal ERMİŞ*

Öz

Günümüzde bilgi teknolojileri çok hızlı bir şekilde ilerlemektedir. Bu gelişmeye paralel olarak iletişim teknolojileri de daha etkin, hızlı ve yaygın bir hale gelmektedir. Bugüne kadar iş hayatında, iletişimde, günlük hayatta vb. bir çok alanda kullanılan klasik iletişim yöntemleri elektronik ortamda da kullanılmaya başlamıştır. Çalışmada, elektronik ortamda kurulan iletişimde, güvenliği sağlamada kullanılan sayısal (dijital) imza incelenmiş ve bu tür teknolojik gelişmelerin belge yönetimine etkisi ele alınmıştır.

***Anahtar sözcükler**: Elektronik imza, Sayısal imza, Onay kurumu, Belge yönetimi, Elektronik belge yönetimi.*

Abstract

Classical communication methods, which have been used extensively in many areas of daily life and amongst especially in business life, started to be used in electronic settings, and at various advanced forms, like digital signature. Digital signature, which aimed primarily at contributing security of communication, was investigated as a specific example of the effects of technological developments on document management.

***Keywords:** Electronic signature, Digital signature, Certification authority, Document management, Electronic document management.*

Giriş

Günümüzde, teknolojik ilerlemeler çağa damgasını vurmuş, her alanda muazzam gelişmeler yaşanmasına olanak sağlamıştır. Internet, söz konusu teknolojik ilerlemelerin en önemli temel taşlarından birini oluşturmaktadır. Artık birçok işlemlerimizi, yazışmalarımızı İnternet aracılığıyla yapabiliyoruz. Bugün; alışverişten bankacılık faaliyetlerine, bilimsel çalışmalardan devlet hizmetlerine kadar her alanda İnternetten yararlanılmaktadır. Bu gelişmeler paralelinde çağımız "bilgi çağı" olarak adlandırılmaya başlanmıştır. Tüm toplumlar da bu çağa ayak uydurup birer "bilgi toplumu" olma yolunda bir dönüşüm-değişim sürecine girmişlerdir.

*TED Ankara Koleji Kütüphanesi; Taşpınar Köyü Yumrubel Mevki Gölbaşı Ankara (kermis@tedankara.k12.tr).

Bu değişim ile birlikte "Bilgi Toplumu'na dönüşüm" ülkeler için önemli bir öncelik haline gelmiş ve e-devlet, e-ticaret, e-sağlık, e-eğitim gibi uygulamalar hızla artmaya başlamıştır. İnternetin çok hızlı gelişmesi sonucunda daha önce başka yollarla yapılan işler elektronik ortamda yapılmaya başlanmış ve bu gelişmelerin doğal bir sonucu olarak elektronik ortamdaki bilgilerin güvenliğinin sağlanması, muhatap olunan kişilerin kimliklerinin tespit edilebilmesi gibi bazı sorunlar da ortaya çıkmıştır. Bu sorunların aşılabilmesini teminen gizlilik, kimlik doğrulama, veri bütünlüğü ve inkar edilemezlik gibi özellikleri haiz olan elektronik imza uygulamasına geçilmiş ve başta gelişmiş ülkeler olmak üzere tüm dünyada bu konuda gerekli olan yasal düzenlemelerin hayata geçirilmesine başlanmıştır (Beydoğan, 2005, s. 42).

Elektronik İmza

Bilgi teknolojisi son derece hızlı bir şekilde gelişmektedir. Posta yolu ile mektup yollamak veya sözleşme akdetmek yakında nostalji olacaktır. Çünkü; iletişim alanındaki teknolojik gelişme gittikçe daha hızlı, etkin ve yaygın hale gelmektedir. Bilgi ağında sadece genel olarak bilgilerin transferi yapılmamakta, bunun ötesinde önemli sözleşmeler, büyük anlaşmalar akdedilmektedir. Hatta tapu sicili gibi kütük kayıtlarının bile gelecekte elektronik olarak yürütülmesi mümkündür. Ancak bunun için, herkese açık olan bu ağ üzerinde yapılacak haberleşmenin güvenilirliğine, güvenliğine ve bağlayıcılığına yönelik olarak acil tedbirler alınması gerektiği vurgulanmaktadır. Sanal ortamda hazırladığımız bir mektup veya bir mesaj nasıl bağlayıcı olacaktır? Şüphesiz bunu hazırlayan kişinin imzası ile! Fakat, bir mesajı veya mektubu elektronik olarak nasıl imzalayabiliriz? Bilgisayar ve İnternetin hayatımızın her alanını işgal etmesi, birbirlerinden kilometrelerce uzakta bulunan kişilerin İnternet üzerinden haberleşmesi, alış veriş yapması veya sözleşme akdetmesi gibi güncel ihtiyaçlar karşısında; kanunlarda yer alan sözleşmelerin şekline ve ispatına ilişkin hükümlerin, bu işlemlerin elektronik yoldan yapılmasına olanak verecek, elektronik iletişimi kolaylaştıracak şekilde yeniden gözden geçirilmesi zorunluluğunu doğurmuştur. Fakat, İnternet üzerinden yapılacak sözleşmelerin geçerli olması ve tarafları bağlaması için, klasik sözleşmelerdeki gibi *"beyan sahiplerinin bu beyanları ile bağlı olma iradelerinin"*, yani sözleşme ile borç altına giren tarafın veya tarafların imzalarının elektronik metinlerde de yer alması gerekmektedir. Sözleşmenin taraflarının elektronik belgeleri nasıl imzalayacakları sorusunun cevabını bulmak ise, yine bilgi teknolojisi uzmanlarına düşmüştür. Bulunan çözüm günümüzde *"elektronik imza"* olarak adlandırılmaktadır (Berber, 2001, s. 12).

Sayısal imza ile elektronik imza kavramları birbirine karıştırılmamalıdır. Elektronik imza, verinin üçüncü tarafların erişimine kapalı bir ortamda bütün-

lüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini, elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir seti ifade eder. Günümüzde kullanılan çeşitli elektronik imza türleri vardır. Örneğin, imza dosyaları, biyometri tekniği ile oluşturulan imzalar ve sayısal imzalar en çok bilinen ve tartışılan elektronik imza çeşitleridir (Elektronik Ticaret Koordinasyon Kurulu [ETKK], 1998, s. 10).

Bir başka tanımda ise, elektronik imza; elektronik ortamda üretilmiş belgelerin imzalanması yöntemlerine verilen genel isimdir. Biyometri tekniği (kullanıcıların parmak ya da el izi, göz retinası vb. kişiye has özellikler) ile oluşturulan imzalar ve sayısal imzalar en çok bilinen ve tartışılan elektronik imza çeşitleridir. Yani sayısal imza, elektronik imzanın türlerinden biridir (Sayısal imza, s. 1) .

5070 sayılı "Elektronik İmza Kanunu*'nda" güvenli bir elektronik imzada bulunması gereken standart unsurlar şöyle ifade edilmiştir:

a) Münhasıran imza sahibine bağlı olan,
b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,
c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,
d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, elektronik imzadır.

Sayısal imzanın yöntem açısından bazı farkları olmasına rağmen temelde veya kullanım amacında elektronik imzadan farklı değildir. Dolayısıyla bu tür konular irdelenirken bu iki kavram birbirleriyle iç içe bir görünüm arz etmektedir.

İmza ve Sayısal İmza

Daha eski çağlardan itibaren, hazırlanan bir mesajın, o mesajı hazırlayan kişiye ait olduğunun üçüncü kişilere karşı ispatı, mesaj sahibinin kullandığı bir ***mühür*** veya ***kaşe*** vasıtasıyla yapılmaktaydı. Aynı şekilde iki taraf arasında yapılacak bir sözleşmede de, sözleşme metninin bu iki kişi arasında bağlayıcı olduğu, tarafların bu metnin içeriği hakkında hemfikir oldukları yine tarafların mühürleri ile tasdik edilirdi. Ancak, bu mühürlerin veya kaşelerin başkaları tarafından elde edilmesi ve kullanılması da oldukça kolaydı. Bu zayıflık, daha o zamanlarda keşfedilmiş ve ortaçağda, kişileri *"son derece mükemmel"* bir şekilde karakterize eden, ***el yazısı ile atılan imza*** mühürlerin yerine geçmiştir. Bir önceki cümlede kullandığımız *"son derece mükemmel"*

* *Elektronik İmza Kanunu: Kanun no: 5070* (23.01.2004). *T.C. Resmi Gazete* (25355), 1-7.

nitelemesi, bilinçli olarak tercih edilmiş bir kavramdır. Çünkü; geçmişte el yazısı ile atılan imzanın başkaları tarafından taklit edilebileceği yolundaki gerekçeler karşısında, bugün konunun uzmanları tamamen farklı görüştedirler ve bu görüşlerini araştırmalarında ve doktrinde çok açık ve şüpheye yer bırakmayacak şekilde ispat etmişlerdir. *"El yazısı ile atılan imza taklit edilemez!"*. Ancak teknoloji hız ve sınır tanımayan bir olgu olduğu için, bütün dünya insanlarını 20. yüzyılda ilk önce ***"İnternet"*** adı verilen küresel ağ ile, daha sonra ise bu ağ üzerinden kendisinden kilometrelerce uzakta bulunan diğer bir kişi ile haberleşmek veya sözleşme yapmak isteyen kişilerin, bu işlemlerini bağlayıcı kılmalarını sağlayacak, kimliklerini ispata yarayacak ***"sayısal (dijital) imza"*** adı verilen bir imza türü ile tanıştırmıştır (Berber, 2001, s. 9).

Sayısal imza, doğrulanan verilerin bütünlüğünü ve imzalayanı tanımlamak için, belirli kural ve parametrelerin birleştirilmesinden oluşan, kriptografi metotlarına dayalı elektronik bir imzadır (Anbar, 2004, s. 11).

Sayısal imza üç temel bileşenden oluşur. Bunlar açık anahtar *(public key),* özel anahtar *(private key)* ve iletişim sırasında aradaki güvenliği sağlayacak sayısal sertifika. Anonim anahtar alıcı tarafına yollanır ve gelen verinin sahibinin ve doğruluğunun tespitinde, özel anahtar ise verinin şifrelenmesinde kullanılır. Bu iki anahtarın birbirinden ayrılarak güvenlik sorununun kesin bir biçimde çözüldüğü söylenilebilir. Sertifika da gönderilen iletinin kime ait olduğunu tescil eder (Mason, 2005, s. 12). Bu sistem yani genel anahtar ile özel anahtarın birbirinden ayrılması Asimetric Kripto Sistem olarak adlandırılmıştır. Bu sistem ilk olarak 1976 yılında Diffie ve Hellman (El-GAMAL) tarafından belirlenen bir teknikle geliştirilmiştir (Doğan, 2001, s.1).

Birçok işlemde kullandığımız imza genel olarak şu amaçlarla atılır:

- **Kanıt:** Bir anlaşmazlığa düşüldüğünde imzalanmış bir belge söz konusu anlaşmazlıkta kanıt olarak kullanılır.
- **Resmiyet:** Herhangi bir kişi bir belgeyi imzaladığı zaman o belge kendisine atfedilir ve resmi bir sıfat kazanır.
- **Onanma:** Hukuki vb. işlemlerde herhangi bir talebin ya da başvurunun onaylanması amacıyla kullanılır.
- **Etkinlik:** Bazı işlemlerimize hız kazandırmak ya da kolaylık getirmek amacıyla da imza kullanılır (Digital …, s. 2).

İmza, kişinin kimliğini teyit ettiği gibi, altına imza atılan metinin okunduğunu, anlaşıldığını, bu metinden kendisine yüklenen birçok sorumluluğun kabul edildiğini ve kendisini hukuken bağladığını teyit eder. Kısacası, imza, atıldığı belgenin her tür sonucunun kabul edildiğini gösterir. Bu belge, mek-

tup, talimat, çek, senet, sözleşme, başvuru formu yahut bunlara benzer her tür belge olabilir. Bu belgelerin farklı şekillerde olması, imzanın niteliğini ortadan kaldırmaz. İmzayla onaylanan her tür belge, her türlü tartışmaya kapatılmıştır. Sayısal imza, nitelik olarak, tükenmez kalemle bir kağıda atılan bildiğimiz imzadan farklı değildir. Yani hukuki bakımdan aynı sonucu doğururlar. Aralarındaki tek fark birinin bir kağıt üzerinde olması, diğerinin de elektronik ortamda bulunmasıdır (Ahi, 2003, s. 2; Gerwig, 2000, s. 14).

Sayısal İmza Türleri

Çeşitli sayısal imza türleri vardır. Tansuğ (2002, s. 4), sayısal imzanın türlerini şöyle sıralamıştır:

- **Kör imza: B**ir kimsenin, bir belgeyi içeriğini görmeden/bilmeden imzalamasına olanak tanıyan dijital imza protokolü.
- **Tuzak imza:** Bir sahtecilik sonucu atılan imzanın sahte olduğunu kanıtlamaya yarayan dijital imza protokolü.
- **Vekalet imzası:** Dijital imza atacak kişiye, kendi gizli anahtarını açmadan bir başkasına imzasını kullandırma hakkı tanıyan dijital imza protokolü.
- **İnkâr edilemeyen imza:** İmzayı atanın rızası olmadan doğruluğu kanıtlanamayan dijital imza protokolü (dijital imzaların kopyalanmasını engellemek için).

Ülkemizde Sayısal İmza Mevzuatı

Ülkemizde elektronik imza yasasının ilk taslağı, Dış Ticaret Müsteşarlığına bağlı Elektronik Ticaret Koordinasyon Kurulu tarafından hazırlanmış ve tartışmaya açılmıştır. Sonrasında Adalet Bakanlığı tarafından yeni tasarı hazırlanmış ve Bakanlar Kurulu tarafından kabul edilen tasarı 9 Haziran 2003 tarihinde TBMM'ye yasalaşması amacıyla gönderilmiş ve meclis komisyonlarından geçerek Genel Kurulda 15 Ocak 2004 tarihinde yasalaşmıştır. 5070 Sayılı e-İmza Yasası, 23 Ocak 2004'te Resmi Gazete'de yayınlandıktan sonra, yasa hükmü gereği 23 Temmuz 2004'te yürürlüğe girmiştir. 6 Ocak 2005'te yayınlanan tebliğ ve yönetmeliklerle yasanın şekillenmesi sağlanmıştır (Tansal, 2005, s. 1).

Ülkemizde elektronik imza mevzuatı genel çerçevede aşağıdakilerden oluşmaktadır:

- TBMM Genel Kurulu'nda 15 Ocak 2004 tarihinde kabul edilip, 23 Ocak 2004 tarihli 25355 Resmi Gazete'de yayımlanan ve yayımından 6 ay sonra, 23 Temmuz 2004 tarihinde yürürlüğe giren 5070 Sayılı **"Elektronik İmza Kanunu"**,

- Elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenleyen, 06 Ocak 2004 Tarihli, 25692 sayılı Resmi Gazete'de yayımlanan "**Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"**,
- Elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirleyen, 06 Ocak 2004 tarihli, 25692 sayılı Resmi Gazete'de yayımlanan "**Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"**,
- 27 Ocak2005 tarihli Resmi Gazetede yayımlanan **"Sertifika Mali Sorumluluk Sigortası Yönetmeliği"** ve ilgili 2005 tarihinde yayımlanan **"Zorunlu Sertifika Mali Sorumluluk Genel Şartları"** ile **"Zorunlu Sertifika Mali Sorumluluk Tarife ve Talimatı"**,
- 6 Eylül 2004 tarih ve 2004/21 sayılı "**Başbakanlık Genelgesi**", Elektronik imza; Türk Ticaret Kanunu, Borçlar Kanunu, Vergi Usul Kanunu, Hukuk Usulü Muhakemeleri Kanunu gibi önemli yasalarla da ilişkilendirilmiş ve yeni hazırlanan tasarılarda da ilgili kanunların, yönetmeliklerin ve genelgelerin kapsamına alınmıştır (Samast, 2005, ss. 1-2).

Sayısal İmzanın Uygulama Alanları

Sayısal imzanın; bankalar ve finans kurumları, şube ağına sahip sigorta şirketleri, kamu kurum ve kuruluşları, holdingler ve diğer büyük şirketler, üniversiteler, yüksek iletişim ve bilgi güvenliği gereksinimi olan organizasyonlar başta olmak üzere orta ve uzun vadede yaygın bir uygulama alanı bulabileceği değerlendirilmektedir. Gerek kamusal gerekse ticari alandaki muhtemel sayısal imza uygulamaları (Elektronik imza, 2004, s. 3) şöyle sayılabilir:

Kamusal Alandaki Uygulamalar

- Her türlü başvurular (ÖSS, KPSS, LES, pasaport vb),
- Kurumlararası iletişim (Emniyet Müdürlükleri, Nüfus ve Vatandaşlık İşleri Müdürlükleri vb),
- Sosyal güvenlik uygulamaları,
- Sağlık uygulamaları (Sağlık personeli - hastaneler - eczaneler),
- Vergi ödemeleri,
- Elektronik oy verme işlemleri,

Ticari Alandaki Uygulamalar

- İnternet bankacılığı,
- Sigortacılık işlemleri,

- ➢ Kağıtsız ofisler,
- ➢ e-Sözleşmeler,
- ➢ e-Sipariş.

Elektronik ortamda yapılacak her tür sözleşme, mektup veya başka tür belgelerin hukuki korunması ancak ve ancak sayısal imza ile mümkün olmaktadır. Sayısal imza, elektronik ortamda üretilen bilgilerin gönderilmesi sırasında göndericinin kimliğini kesinlikle teyit edecek, verinin başkası tarafından gönderilmediğini garanti edecek ve bu verilerin güvenliğini sağlamak amacıyla gizliliği esas alacak ve başkası tarafından değiştirilemeyecek bir uygulamadır. Sayısal imza, bir imzacının imzalanacak metnini şifreleme ve sıkıştırma mantığı ile çalışan, açık ve gizli iki anahtarlı kriptoloji tekniği ile sayısal karakterlere dönüşmüş özetini şifreli olarak belge altına eklemesidir. Ancak, bu işlem tek başına yeterli olmamakta birde arada onay makamı denilen ve kimlik doğrulaması yapan bir kuruluş bulunmaktadır. Bu kuruluş genel olarak "Sertifikasyon Otoritesi", "Onay Makamı" ya da "Onay Kurumu" olarak adlandırılmaktadır (Ahi, 2003, s.4).

Sayısal İmzanın Yararları

Sayısal imza, bir takım faydaları ile ön plana çıkmaktadır. Bunlar:

- ➢ Sayısal imza veri bütünlüğünü sağlar. Sayısal imza, doküman ve mesajın değiştirilmediğinin ve karıştırılmadığının bir kanıtını oluşturmaktadır.
- ➢ Sayısal imzanın diğer bir üstünlüğü, kimliklerin belirlenmesinde ortaya çıkmaktadır. Sayısal imza, alıcı ve göndericinin kimliğini tanımlamayı kolaylaştırmaktadır.
- ➢ Sayısal imzanın önemli bir üstünlüğü de, inkar edilememesidir. Bunun anlamı, ne gönderici gönderilen mesajı göndermediğini, ne de alıcı, gönderilen veya alınan mesajı almadığını inkar edemezler.
- ➢ Sayısal imza, otomatik tarih ve zaman pulu içermektedir. Bu, ticari işlemlerde büyük bir önem arz etmektedir.
- ➢ Sayısal imza, işlemlerin hızını ve doğruluğunu artırmaktadır. Örneğin bir banka, binlerce sayısal imzayı el imzasına göre daha hızlı kontrol edebilir.
- ➢ Şifreleme sistemi kullanıldığı için daha güvenlidir (Anbar, 2004, s. 13).
- ➢ İmzalanması için kullanılan gereksiz kağıt israfını ve kırtasiye masraflarını azaltmaktadır.
- ➢ Basılı kağıtların dosyalanması, depolanması gibi işlemlerinde kolaylıklar sağlayarak gereksiz yer işgalini en aza indirmektedir (Gupta, Tung ve Marsden, 2004, s. 564).

Sayısal İmzada Onay Kurumu

Birbirleri ile haberleşen her iki tarafın kimliklerinin belirlenmesi ve aralarındaki iletişimin güvenli bir şekilde sağlanması için üçüncü bir kuruma ihtiyaç vardır. Aradaki iletişimin denetimli bir şekilde devam edebilmesi için bu kurumların sayısal sertifika düzenlenmeleri gereklidir. Bu sertifikaları düzenleyen kurumlar "Onay Kurumu", "Elektronik Sertifika Hizmet Sağlayıcısı" ya da "Onay Makamı" vb. isimlerle adlandırılmaktadır.

Sayısal sertifika ve onay kurumu ile ilgili bazı tanımlamalar şöyledir;

- Sayısal Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır (Bilgi ..., s. 1).
- Başka bir tanımda ise sayısal sertifika; başvuran kişinin adını, seri numarasını, açık anahtarını, belge kontrat bilgilerini içeren onay kurumu tarafından hazırlanan sayısal bir dokümandır (Moore, 2001, s. 2).
- Onay kurumu**;** kullanıcılarına kendi şifrelerini oluşturmalarına olanak veren sonra da gerektiğinde bilgisayar ortamında şifreli bir iletişim kurabilmelerine yarayan sayısal sertifika sağlayan kurumdur (Kuechler ve Grupe, 2002, s. 27).

Başka bir tanımda ise; Elektronik Sertifika Hizmet Sağlayıcısı (onay kurumu): Elektronik Sertifika Hizmet Sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel tüzel kişilerdir.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

- Güvenli ürün ve sistemleri kullanmak,
- Hizmeti güvenilir bir biçimde yürütmek,
- Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak, ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir. Her sertifika hizmet sağlayıcısı, başvuruları doğrulamak için gereken metotları anlatan Sertifika Uygulama Esasları (SUE) ve Sertifika İlkeleri (Sİ) adlı belgeleri sağlamalıdır (Elektronik imza, 2004, s. 3).

Nitelikli bir elektronik sertifikada (Elektronik İmza Kanunu, 2004);

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,
- Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,
- İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,
- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

- ➢ Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,
- ➢ Sertifikanın seri numarasının,
- ➢ Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,
- ➢ Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin,
- ➢ Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin,
- ➢ Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının bulunması zorunludur.

Onay kurumu *(Certification Authority-CA),* kayıtlı kullanıcı olarak adlandırılan kişinin tanımlanmasını sağlayan ve kişinin kendisine ait sayısal imza oluşturmak için kullandığı açık-gizli anahtar çiftinden, açık anahtarı onaylayan güvenilir üçüncü taraftır. Sertifika veya diğer bir adıyla elektronik kimlik belgesi ise, güvenilir üçüncü taraf (onay kurumu) tarafından imzalanan ve kullanıcıyı tanımlayan verileri içeren bilgisayar bazlı bir kimlik belgesidir. En yaygın sertifika formatı, ASN.1 dilinde olan ve *Consultative Commitee for International Telegraph and Telephone* (CCITT) tarafından tavsiye edilen, X.509'dur. X.509 sertifikası, kullanıcı hakkında standart bilgileri (kullanıcının adı, çalıştığı kurum, e-posta adresi, kullanıcının açık anahtarı, sertifikanın veriliş tarihi ve geçerlilik süresi vb.) içermektedir. Bu sertifikaya, kullanıcının kimliğini doğrulamak isteyen herkes ulaşabilmektedir. Kullanıcı, dokümanı kendi gizli anahtarıyla imzalayıp alıcıya gönderdiğinde, alıcı, X.509 veri bankasından gönderenin sertifikasını arayıp bularak, göndericinin kimliğini doğrular. Ayrıca, alıcı, sertifika iptal listesini (*Certificate Revocation List*-CRL) kontrol ederek, gönderenin sertifikasının iptal edilip edilmediğini sorgulayabilir. CRL, sona erme tarihlerinden önce iptal edilen sertifikaların kayıtlı olduğu basit bir veri bankasıdır. Genellikle bu hizmet, onay kurumu tarafından verilmektedir. Kişi öldüğünde, gizli anahtarı kaybolduğunda veya çalındığında, kullanıcının bilgileri değiştiğinde ve diğer nedenlerden dolayı, kişinin sertifikası bu listeye alınır (Anbar, 2004, s. 6).

Onay kurumu kullanılan sayısal imzayı doğrulayarak söz konusu elektronik dokümanın kime ait olduğu açık bir şekilde ortaya koyar. Bununla beraber bu belgenin güvenliğini sağlayarak başka birinin izinsiz erişimini engeller (Freeman, 2004, s. 9).

Elektronik Sertifika Hizmet Sağlayıcıları'nın Yükümlülükleri Nelerdir?

- ➢ Güvenli ürün ve sistemleri kullanmak.
- ➢ Hizmeti güvenilir bir biçimde yürütmek.

- ➢ Nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek.
- ➢ Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, mesleki veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmi belgelere dayandırarak güvenilir bir biçimde belirlemek.
- ➢ İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamak.
- ➢ Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmek.
- ➢ Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmek.
- ➢ Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle (örneğin 20 yıl) saklamak.
- ➢ Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak.
- ➢ Telekomünikasyon Kurumunun belirleyeceği ücret alt ve üst sınırlarına uymak.
- ➢ Hizmetin gerektirdiği nitelikte personel istihdam etmek.
- ➢ Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmek.
- ➢ Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal etmek.
- ➢ Nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturmak. Böylece üçüncü kişilerin iptal edildiğini bilmedikleri bir sertifikaya güvenerek işlem yapmalarından dolayı bir zararın doğması önlenmiş olacaktır.
- ➢ Faaliyetine son vereceği tarihten en az üç ay önce durumu kuruma ve elektronik sertifika sahibine bildirmek.

- ➢ Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.
- ➢ Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez.
- ➢ Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz.
- ➢ Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz (Civelek, 2004, s. 4).

Bu konuda uluslararası platformdaki tartışmalar sonuçlandırılmamış olmakla birlikte, en üst seviyede bir yetkili bir makam (üst onay makamı) tarafından belirlenen koşullarda hizmet veren ve bu koşullara uygun hareket etmekle sorumlu olan bağımsız, özel onay makamlarından oluşturulmuş bir yapı kurulmasında yarar görülmektedir. Onay makamlarınca yerine getirilecek işlevler (kimlik doğrulama ve sayısal imza anahtarı bilgilerinin saklanması) elektronik işlemlerin gelişmesi açısından son derece önemli olmakla birlikte, onay makamlarının kişisel bilgilere ve taraflarca yapılacak iletişime ulaşma olanağı sağlayacak bilgileri bünyelerinde barındırmaları söz konusu olduğundan, onay kurumları sisteminin dikkatle ele alınıp düzenlenmesinde yarar görülmektedir. Ayrıca elektronik ticaretin gelişmesinde özel sektör öncülüğü ilke olarak benimsendiğinden, üst onay makamının idari altyapısında özel sektör temsilcilerine de yer verilmesini sağlayacak bir yarı kamusal statü de düşünülmelidir. Sisteme duyulan güveni azaltma endişesi yaratacak olmakla birlikte, kamu güvenliğini gerektiren durumlarda veya suç örgütlerinin ya da benzeri gizli faaliyetlerin izlenmesinde istihbarat amaçlı olarak, bazı yetkili devlet birimlerinin kullanıcıların gizli anahtarlarına ulaşabilmelerine imkan tanıyan bir yasal altyapı oluşturulabilir. Ancak, bu istisnai uygulamalar dikkatle düzenlenmeli ve mümkün olduğu kadar sınırlı tutulmalıdır. Diğer taraftan, böyle bir uygulamanın gerçekleşebilmesi için, kullanıcılara ait gizli anahtarların onay makamlarının veri bankalarında saklanması gerekecektir. Bu durumda, onaya makamlarının ya da söz konusu veri bankasına ulaşabilecek yetkisiz tarafların kişisel bilgilere ve her türlü elektronik iletişime erişmeleri tehlikesi ortaya çıkacaktır. Bu tür izinsiz erişimlerin önlenebilmesi için gerekli tedbirler mutlaka sisteme eklenmeli ve caydırıcılık sağlanmalıdır (Özyılmaz ve Evsenel, 2000, s. 5).

Elektronik İmza Neden Yaygınlaşmıyor

Giriş bölümünde ifade edildiği gibi, yasaların tamamlanmasına karşın elektronik imzanın yaygın kullanımı henüz yoktur. Bunun nedenleri pek çok farklı etmene bir arada bağlı olabilir. Burada, daha çok açık anahtarlı altyapı teknolojilerine ilişkin etmenler üzerinde durulacaktır:

- Teknolojiden kaynaklı uygulama güçlükleri: Anahtar ve sertifika üretimi, dağıtımı, yenilenmesi, iptali, genel olarak anahtar ve sertifikaların yönetilmesi karmaşık bir süreçtir. Sertifika hizmet sağlayıcıları, sertifika yönetimi altında sertifika başvurularının gerçekleştirilmesi, sertifikaların üretilmesi, yenilenmesi, yayınlanması, gerek duyulduğunda iptal edilmesi ve tüm bu işlemlere ilişkin ayrıntılı kayıtları tutmak durumundadır. Sertifika başvurularının güvenilir bir biçimde yapılmasının sağlanması, gerçek kişilere doğru sertifikaların verilmesinde son derece önemlidir. Sertifika üretim süreci, azami fiziki, teknik ve idari güvenlik içinde gerçekleştirilmelidir. Hizmet sağlayıcının gizli anahtarına izinsiz erişim, telafisi güç sorunlara neden olur. Sertifikalar yaşayan bir sistemin en önemli unsurlardır. Genellikle bir yıl geçerlilik süresi verilen sertifikaların, süresi tamamlanmadan önce aynı anahtar çiftiyle yenilenmeleri veya yeni bir sertifikanın alınmasına ihtiyaç olacaktır. Süresi içinde olmasına karşın, bir sertifikanın çok farklı nedenlere dayalı iptali gerektiğinde, bu zaman yitirmeden ve güvenli bir biçimde hizmet sağlayıcı tarafından yapılabilmelidir. Sertifika sahiplerinin gizli anahtarlarını korumaları için yeterince bilinçli olmaları, uygun araçları bu amaçla kullanmaları ve sistemin işleyişine ilişkin genel de olsa bilgi sahibi olmaları gerekmektedir. Aksi halde, imzadan doğacak yasal sorumlukların işletilmesinde ciddi sorunlarla karşılaşılabilir.
- Uyumluluk sorunları: Sayısal imza elektronik uygulamalarda güvenliği sağlamak üzere geliştirilmiş bir araçtır. Birbirleriyle ilişkisi olmayan çok farklı uygulamalarda güvenliğin sayısal imzayla sağlanması söz konusudur. Uygulamalar arasında uyumlu entegrasyon için, sayısal imzalara ilişkin standartların tam olarak yerleşmiş olması zorunludur. Daha zorlu bir sorun, sayısal imzanın kendisiyle ilişkilidir. Sayısal imza, matematiksel olarak tanımlanmış olmasına karşın, uygulamalarda imzanın imzalanmış veriyle birlikte nasıl oluşturulacağı, nasıl taşınacağı ve nasıl korunacağına ilişkin yerleşmiş bir standart henüz bulunmamaktadır. Bu durumda, birbirinden bağımsız taraflarca imzalanmış farklı belgelerin diğer taraflarca sağlıklı bir biçimde doğrulanmasında güçlükler yaşanması kaçınılmazdır. Benzer bir sorun, sertifikanın ve gizli anahtarın taşınabilir olmasını

sağlayan ve gizli anahtarın korunması için güvenilir bir araç olarak bilinen akıllı kartlara ilişkin bulunmaktadır. Akıllı kartların kullanımı, bilgisayara dışarıdan bir akıllı kart okuyucusunun tanıtılmasıyla mümkündür. Akıllı kart okuyucuları belli bir kurulum programı gerektirmekte, işletim sistemine hatta aynı işletim sisteminin farklı sürümlerine bağlı olarak çalışmaktadır. Bilgisayar kasasında standart bir sürücü olarak yer almaması, okuyucuların kullanım kolaylığı açısından başka bir sorundur. Hareket halinde olan bir kullanıcı için gittiği her yerde okuyucu bulabilmesi veya okuyucusunu beraberinde (gittiği her yerde kurulum yapmak üzere) taşıması kullanımı güçleştirmektedir. Daha da güç olanı, belirlenmiş standartların yetersiz gerçekleştirimleri sonucu kimi durumlarda her kartın her okuyucuyla birlikte uyumlu olmamasıdır. Dikkat çekilebilecek diğer önemli bir uyumluluk sorunu zaman damgasıyla ilişkilidir. Elektronik bir sözleşmenin ayrılmaz zorunlu bir parçası olmakla birlikte, zaman damgasının henüz genel kabul görmüş bir standardı bulunmamaktadır.

- Bilgi ve bilinç eksikliği: Açık anahtarlı sayısal imza teknolojilerinin yaygınlaşmasının önündeki diğer bir engel, potansiyel kullanıcı kitlesinde belirli düzeyde bir bilgi birikimi gerektirmesidir. Teknolojinin karmaşıklığı nedeniyle kullanıcı, bilinçli bir kullanım düzeyi için en azından sertifika hizmet sağlayıcısının uygulama ilke ve esasları hakkında bilgi sahibi olmalıdır. Aksi takdirde, elektronik imza kanunuyla kendisine yüklenmiş sorumlulukları taşımasında güçlükler olacaktır. İmzanın olası ağır ve bağlayıcı sonuçlarıyla birlikte teknolojinin karmaşıklığı ve kullanım güçlüğü bir araya geldiğinde, kullanıcının gerçekten istekli, bilinçli ve bilgili olması zorunlu hale gelmektedir.
- Yüksek uygulama maliyetleri: Açık anahtarlı sayısal imza teknolojileri yüksek maliyetli bir uygulamadır. Sertifika hizmet sağlayıcısı, sistemin gerektirdiği güvenliği sağlamak üzere bina, yazılım, donanım ve iletişim altyapısı yatırımı yapar; hizmette beklenen kaliteyi sağlamak üzere yüksek işletme giderleriyle karşı karşıya kalabilir. Bir yanda yasaların öngördüğü standartları yakalamak üzere çalışırken öte yanda rekabetçi bir ortamda yaşayabilmek için yüksek pazar payı elde etmeye çalışır. Sertifika kullanıcıları, kart, okuyucu ve token gibi yazılım ve donanım gereksinimlerinin yanı sıra, sertifikalara da belli bir ücret ödemek durumundadır. Sertifikadan sertifika sahibine veya diğer kişilere doğabilecek zararlar için mali sorumluluk sigortası yaptırılması bir zorunluluktur. Bu durumda sertifika maliyetleri daha

da artar. Sertifikaların geçerlilik süresi sonunda yenilenmeleri, iptal durumlarında yenilenmeleri diğer ek maliyet unsurlarıdır (Tüfekci, 2002, ss. 3-4).

Yabancı Ülkelerde Sayısal İmzanın Hukuki Altyapısı ve Gelişme Süreci

Çok genel bir ifadeyle, dünyada elektronik imzalarla ilgili yasaların ikiye ayrıldığı, bazı yasaların ABD örneğinden hareketle "minimalist" yaklaşım içinde, diğerlerinin ise "Açık Anahtar Altyapısı"na dayalı elektronik imzalara hukuki netice bağlanması şeklinde bir görüş çerçevesinde hazırlandığı belirtilebilir. Çeşitli ülkelerde yürürlükte olan ve son aşamasına gelmiş yasalara geçmeden önce, ABD ve AB'de elektronik ticaretin temelini teşkil eden hukuki mevzuattan ve UNCITRAL (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu) model yasalarından kısaca bahsetmek yararlı olacaktır (Demirel, 2006, s. 1) :

1. ABD'de elektronik imzaların hukuki statüsü esas olarak üç kanunla belirtilmiştir.

a) Standart Elektronik İşlemler Yasası, model yasa olarak otuz kadar eyalet tarafından kabul edildi ve eyalet yasalarına göre elektronik imza kullanımı için temel çerçeveyi çizmektedir.

b) Ulusal ve Uluslararası Ticarette Elektronik İmza Yasası (E-İmza), ulusal çerçevede esasları belirtmektedir.

c) Devlette Kırtasiyenin Azaltılması Hakkında Yasa, kamu kurumlarına elektronik kayıtları ve imzaları kullanımda belirli yükümlülükler getiren federal bir yasa.

2. AB'de elektronik ticaret ve elektronik imza ile ilgili iki esas direktif bulunmaktadır.

a) 8 Haziran 2000 tarihli, 2000/31 AB sayılı, Elektronik Ticaret Direktifi, bilgi toplumu hizmetlerinin üye ülkeler arasında serbest dolaşımını sağlamak amacıyla hazırlanan bu direktifte elektronik sözleşmeler ve bunların hukuki neticelerine ilişkin önemli hususlar bulunmaktadır.

b) 13 Aralık 1999 tarihli, 1999/93 AB sayılı Elektronik İmza Direktifi. AB üyesi ülkelerin bu direktife uyum sağlamak üzere gerekli yasa, düzenleme ve idari hükümleri yürürlüğe koymalarını şart koşmaktadır. Direktifin amacı elektronik imzanın kullanılmasını kolaylaştırmak ve hukuken tanınmalarına katkıda bulunmak şeklinde belirlenmiştir. Elektronik imza sertifikaları, sertifika hizmet sağlayıcıları, bunların gözetimi ile ilgili esaslar bu direktifte yer almaktadır.

3. UNCITRAL tarafından ülkelere yasa hazırlanmasında örnek olmak üzere iki model yasa hazırlanmıştır;

a) 1990 tarihli Model Elektronik Ticaret Yasası, elektronik verilerin ve sözleşmelerin hukuken tanınmasına ilişkin hükümler içermektedir.

b) 2001 tarihli Elektronik İmzalara İlişkin Standart Hükümler, elektronik imzalarla ilgili genel esasları belirtmektedir (Demirel, 2006, s. 1).

Bu uygulamalar, dünyada henüz gelişme aşamasındadır ve bu açıdan önde sayılabilecek ülkelerden biri Güney Kore'dir. Güney Kore'nin nüfusu yaklaşık 48 milyon, satın alma gücü paritesiyle düzeltilmiş kişi başı milli geliri yaklaşık 15.000 ABD doları (Türkiye'nin yaklaşık 3 katını), her 10 evden 7'sinde geniş bant İnternet erişimi, benzer bir biçimde nüfusun %70'inde cep telefonu bulunmaktadır. Güney Kore elektronik imza kanununu 1999 yılında çıkarmış; 2001 yılında önemli değişikliklere gitmiştir. 2003 yılında ilki kadar kapsamlı olmasa da bir değişiklik daha yapılmıştır. 2000 yılından başlayarak 6 elektronik sertifika hizmet sağlayıcısı faaliyete geçmiş ve her biri milyonlarca dolar yatırım yapmıştır. 2000 yılında 50 bin ile başlayan sertifika sahibi sayısı, 2003 itibariyle 7 milyona ulaşmıştır. Güney Kore için çarpıcı istatistikler arasında, yaklaşık 18 milyon İnternet bankacılığı kullanıcısı olduğunu ve borsa işlemlerinin %64'ünün ağlar üzerinde gerçekleştiğini de saymak gereklidir (Tüfekçi, t.y., ss. 5-6).

Diğer çarpıcı bir örnek olan Almanya'da, Elektronik imza konusu, Avrupa Topluluğu'nun sözünü ettiğimiz bu Yönergesinden daha önce, 13 Temmuz 1997 tarihinde *"Bilgi ve İletişim Hizmetleri Kanunu*"nun 3. paragrafında Alman Parlamentosu tarafından kanun (Dijital İmza Kanunu) olarak kabul edilmiştir. Almanya'da bu kanundan başka, ayrıca 8 Ekim 1997 tarihli bir de Dijital İmza Yönetmeliği yürürlüktedir. Almanya bu kanun ile, dünyadaki birkaç devletten biri olarak dijital imzanın uygulanması için çok önemli bir yasal dayanak yaratmıştır (Berber, 2001, s. 15).

ABD ise, 2000 yılında elektronik imzayı federal düzeyde yasalaştırmıştır. ABD'de 90'lı yılların ikinci yarısıyla birlikte elektronik sertifika hizmet sağlayıcıları faaliyete geçmiştir. Aynı zamanda federal düzeyde hizmet veren bir kamu elektronik sertifika hizmet sağlayıcısı da bulunmaktadır. Bir ana kök işlevi üstlenen kurum, tüm ABD'de kamusal alanda elektronik sertifika kullanımının sağlanmasında anahtar rol oynar. ABD yönetimi, bu yasayla beraber kamuda kağıt kullanımını azaltmayı da hedeflemiş durumdadır. Özellikle güvenli web sunucularında önemli bir pazar oluşmasına karşın, kişisel sertifika kullanımı için aynı şey geçerli değildir. (Tüfekçi, t.y., s. 6).

Bu genel çerçeveden sonra, çeşitli ülkelerdeki elektronik imza ve ticaret konusundaki yasalar ve yürürlüğe girdikleri tarihler aşağıda gösterilmektedir:

AB Üyesi Ülkeler

- **Belçika:** 14 Haziran 2001 tarihinde sertifika servisleri ve Elektronik İmzaların Hukuki Çerçevesinin Esasları Hakkında Yasa yürürlüğe girdi.
- **Danimarka:** 1 Ekim 2000 yılında Elektronik İmzalar Hakkında Yasa yürürlüğe girdi.
- **Fransa:** İki ayrı yasa vardır. Mart 2000 tarihli, 2000-230 sayılı yasada, elektronik imza ve belgelere, ispat konusunda kağıda dayalı belgelere benzer esaslar getirmektedir. 2001 tarihli, 2001-272 sayılı yasa ile AB direktifinde yer alan hususların çoğu tanınıyor.
- **Yunanistan:** Bu konularla ilgili kanunlar hazırlanıyor, ancak kesinleşmedi.
- **İtalya:** AB direktifini henüz yürürlüğe koymadı, ancak Mart 1997 tarihli, 59 sayılı yasa ve 1997 tarihli kararname ile Açık Anahtar Altyapısı (PKI) esasına dayanan, sayısal imzalarla ilgili esasları tanıdı. Bunlar AB direktifinden önemli konularda ayrılıyor.
- **Hollanda:** AB direktifiyle uyumlu bir kanun 2002'de yürürlüğe girdi.
- **Lüksemburg:** 14 Ağustos 2000 tarihli E-Ticaret Yasası, AB direktifiyle uyumlu.
- **İsveç:** 1 Ocak 2001'de yürürlüğe giren Nitelikli Elektronik İmza Yasası, AB direktifiyle uyumlu.
- **Portekiz:** Ağustos 1999 tarihli, 290-D/99 sayılı yasa elektronik imza ve elektronik belgelerin geçerliliği hususunda esasları belirtmektedir.
- **İspanya:** 17 Eylül 1999 tarihli Elektronik İmza Yasası ile AB direktifini yürürlüğe koydu.
- **İngiltere:** 2000 tarihli Elektronik Komünikasyon Yasası elektronik imzaların kullanımı ve hukuki geçerliliği ile ilişkili.
- **İrlanda:** 10 Temmuz 2000 tarihli Elektronik Ticaret Kanunu, elektronik imzayı ve kayıtları düzenliyor.
- **Avusturya:** Federal Elektronik İmza Kanunu, 1 Ocak 2000'de yürürlüğe girdi.
- **Estonya:** 15 Aralık 2000'de yürürlüğe giren Sayısal İmza Yasası var.
- **Malta:** Mayıs 2000'de yayımlanan bir raporda, Elektronik Ticaret, Veri Korunması ve bilgisayarların kötüye kullanılmasına ilişkin 3 yasa hazırlanması öngörülüyor. (Kırçova, 2003, s. 79)

Diğer Avrupa Ülkeleri

- **Çek Cumhuriyeti:** Elektronik İmza Yasası 1 Ekim 2000'de yürürlüğe girdi. Bu yasa, AB direktifiyle uyumlu.
- **Macaristan:** Elektronik İmza Yasası 1 Eylül 2001'de yürürlüğe girdi. AB direktifiyle uyumlu.
- **Polonya:** Elektronik İmza Yasası Temmuz 2000'de yürürlüğe girdi.
- **Bulgaristan:** Elektronik Belgeler ve Elektronik İmza'ya ilişkin bir taslak meclise sunuldu ve kabul edildi.
- **Slovakya:** Elektronik İmza Yasası'nın hazırlanmasına yönelik bir çalışma grubu teşkil edildi ve çalışmalar sürüyor.
- **Slovenya:** 22 Ağustos 2000'de Elektronik Ticaret ve Elektronik İmza Yasası yürürlüğe girdi.
- **İzlanda:** Nisan 2001 tarihli Elektronik İmza Yasası kabul edildi.
- **Norveç:** Elektronik İmzaların Kullanımı ve Tanınması Hakkında Yasa Temmuz 2001'de yürürlüğe girdi. AB direktifiyle uyumlu.
- **Ukrayna:** Elektronik belgelere ilişkin yasasını çıkardı, UNCITRAL Model Yasası esas alınmış. (Demirel, 2006, s. 2)

Amerika

- **Kanada:** Tüm elektronik işlemlerle ilgili olarak 10 Nisan 2001'de yürürlüğe giren Elektronik İşlemler Yasası var.
- **Arjantin:** 15 Ağustos 2001 tarihli Sayısal İmza Kanunu var.
- **Bermuda:** 1999 tarihli Elektronik İşlemler Yasası, elektronik imza ve kayıtları kapsıyor.
- **Brezilya:** Sayısal imzalarla ilgili 1999 tarihli bir taslak yasa var.
- **Kolombiya:** 21 Ağustos 1999 tarihli, 527 sayılı Elektronik Ticaret Yasası var. 1996 tarihli UNCITRAL Model Elektronik Ticaret Yasası örnek alınmış.
- **Ekvator:** Elektronik ticaret, elektronik imza ve veri mesajlarını kapsayan bir taslak hazırlandı.
- **Meksika:** Ticaret kanununda elektronik imzaları kapsayacak bir değişiklik yapılmak isteniyor (Tansuğ, 2002, s. 12) .

Asya

- **Japonya:** 24 Mayıs 2000'de kabul edilip, 1 Nisan 2001'de yürürlüğe giren Elektronik İmzalar ve Sertifika Hizmetleri Hakkında Yasa.
- **Singapur:** 29 Haziran 1998 tarihli Elektronik İşlemler Yasası.
- **Çin Cumhuriyeti:** İnternet bankacılığına ilişkin yasal düzenlemeler var.

- **Rusya:** 1995 tarihli Rusya Federasyonu Bilişim Yasası, elektronik imzalara ilişkin.
- **Malezya:** 1 Ekim 1998 tarihinde Sayısal İmza Yasası yürürlüğe girdi.
- **Tayvan:** Elektronik İmza Yasası yasalaşma süreci içine girdi.
- **Tayland:** Elektronik İşlemlerle ve Elektronik İmzalarla ilgili iki yasa taslağı birleştirildi ve taslak kabine tarafından onaylandı (Demirel, 2006, s. 2).
- **Hindistan**: Sayısal teknoloji konusunda Hindistan'da 2000 yılında "Hindistan Bilgi Teknolojileri Kanunu" onaylanmıştır. Bu kanunla, Hindistan, şifrelemede kullanılan anahtar çiftinin kullanıcılar tarafından belirlenebildiği 4 ülkeden biridir (Srivastava, 2005, s. 399).

Günümüzde elektronik ticaret oranları gittikçe artmakta ve bu kavram her geçen gün değer kazanmaktadır. Birçok şirket bu alanda hizmet vermektedir. Dolayısıyla elektronik alandaki bilgilerinin güvenliğini daha etkili bir düzeyde sağlayacak önlemlere ihtiyaç duymaktadırlar. Yasal sorumluluklar yüklenen sertifika sağlayıcılar, güvenliği ve gizliliği sağlama yolunda önemlidirler (Zaba, 2006, s. 25). Sertifika sağlayıcılarının gereksinim duyulan güveni sağlamak amacıyla kullandığı yöntemlerden biri olan sayısal imza giderek daha önemli hale gelmektedir.

Sayısal imzanın günlük elektronik hayatımıza gireceği ve doğal bir unsuru olacağı konusunda yalnız uzmanlar değil, birçok kimse hem fikirdir. Çünkü; güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden bahsetmek mümkün değildir. Bu ihtiyaç sadece şirketler, kurum veya kuruluşlar için değil, aksine *chip* kartta bulunan imzasını kullanarak siparişler veren, banka işlemlerini evinden halletmek isteyen veya İnternette sadece sörf yapmak yerine hukuken bağlayıcı işlemler yapmak isteyen gerçek kişiler bakımından da söz konusudur (Berber, 2001, s. 51).

Sayısal imza uygulaması elektronik ortam üzerinden yapılan veri alışverişlerinin güvenliği açısından en önemli açığı kapatan sistemdir. Sayısal imzaları oluşturan algoritmaları çözebilmenin neredeyse imkansız olduğu bilimsel çevrelerce kabul edilmektedir. Gelişmiş birçok ülkede İnternetin günlük hayatta çok aktif kullanımı dolayısıyla yapılan büyük çalışmalar sonucu elde edilen bu sistem aynı ülkeler tarafından resmi olarak tanınmakta ve imza sahipleri de imzalarının yer aldığı tüm dijital dokümanlardan sorumlu tutulmaktadırlar. Bu sayede İnternet üzerinden yapılan ticari anlaşmalar ve bilgi alışverişinin güvenliği sağlanmış ve insan hayatını büyük ölçüde kolaylaştıran bilgisayar ve İnternet ortamının kullanımındaki sorunların büyük ölçüde önüne geçilmiştir. İçinde bulunduğumuz teknolojik altyapı ve kaynaklar bu şekilde üretilen imzaların taklit edilmesinin imkansızlığını ortaya

koymuştur. Sayısal imza İnternet ortamında kişisel güvenliği en iyi seviyede sağlayan yöntemlerden biridir.

Elektronik Belge Yönetiminde Sayısal İmza

İnsanlar artık geçmişe oranla her geçen gün daha çok bilgiye, daha farklı yöntemlerle, sesli görüntülü, elektronik, basılı vb. dosyalara ulaşmaktadırlar. Her gün okumak durumunda kaldığımız yazışmalar, e-postalar, raporlar, dinlemek ve cevaplamak zorunda kaldığımız diyaloglar, telefonlar artan kurumsal çalışmalara örnek olarak gösterilebilir. Bütün bu faaliyetler sonucunda kurumlar, yoğun bir bilgi ve belge üretimi ile karşı karşıya kalmışlardır (Odabaş, 2003, s. 358).

20. yüzyıl'ın ikinci yarısından itibaren bilgi teknolojilerinde meydana gelen hızlı ilerleme ve gelişme her meslek sahasında olduğu gibi belge yönetimi alanında da ciddi bir değişime ve dönüşüme neden olmuştur. İlerlemenin gereği olarak bu değişime ayak uydurmak mesleki gelecek açısından çok önemlidir. Belge yöneticileri; işlerini daha etkili ve yeterli yapabilmelerine olanak sağlayan bilgi teknolojilerini iyi anlama ve gereklilikleri açısından kendilerini yetiştirmek durumundadır. Bilgi teknolojileri, kağıt belge dışında yönetilmesi gereken belge türlerinin oluşmasına yol açmıştır. Kağıt belge etrafında şekillenen geleneksel belge yönetimi bu yeni durumla birlikte, yeni yaklaşımlar ve çözümler ortaya koymak durumunda kalmıştır. Yeni belge türü olarak elektronik belgelerin yönetilmesinde, kağıt belgelerin yönetiminde uygulanan yöntemlerde aynı şekilde uygulanabilmektedir. Ancak özellikle saklama ve yaşam süreçleri konusunda elektronik belgeler farklılık göstermektedir. Bu bağlamda bir elektronik belge aynı anda farklı yaşam süreçlerinde bulunabilmektedir. Yani elektronik bir belge aynı anda aktif ve yarı aktif olabilmektedir. Elektronik belgeler yönetilirken bu durum göz önünde bulundurulmalıdır. Çünkü önemli bir belge yanlış bir yaşam sürecinin tercihi sebebiyle ulaşılamaz hatta değersiz bir belge haline gelebilmektedir. Bilgi teknolojilerindeki gelişmelerin beraberinde getirdiği bu ve benzeri sorunlar mesleki değişimi kaçınılmaz hale getirmiştir (Aydın, 2005, s. 90). Öncelikle, bu konuyla ilgili kavramların ne olduğuna bakmak gerekir;

Belge: İşlemlerin veya yasal zorunlulukların yerine getirilmesinde bir kişi veya organizasyon tarafından enformasyon ve delil olarak üretilen, kabul edilen (alınan) ve korunan enformasyondur (Özdemirci, 2004, s. 194).

Belge yönetimi; belgelerin, üretiminden son düzenlenmesine kadar sistematik bir kontroldür. Böyle bir sistematik yaklaşım; bir kurumda artan kırtasiyeyi azaltmak, bilgi ve belge isteklerine etkin erişim sağlamak, güncelliğini yitiren belgeleri depolamak, devletin tüm kurumlarının dokümantasyon

gereksinimlerini karşılamak ve kurumların tarihi kayıtlarını korumak gibi belgelerin yaşamının tüm aşamalarını kontrol etmek için gereklidir. Kurumların başarısının devamı için bilgi gittikçe daha fazla önem kazanmıştır. Kurumlarda bilgi herhangi bir ortam üzerine kayıtlı bir belge olarak ortaya çıkmıştır. Bu nedenle belgeler kurumların çok önemli temel bilgi kaynakları olmuş ve ona bağımlılıkları sürekli olarak artmıştır. Bu temel kaynağın yönetimi için bir sistem oluşturmak zorunluluğu da kendiliğinden ortaya çıkmıştır. Belgelerin üretimi, planlaması, organizasyonu ve kontrolü için geliştirilen bu sistem belge yönetimi olarak bilinmektedir. Belgelerin üretimi, işlemleri, depolanması, erişimi, dağıtımı, kullanımı ve tasfiyeleriyle ilgili olan belge yönetimi; yazışmalar, formlar, raporlar, talimatlar, postalama ve kopyalama yönetimi gibi özel gereksinimleri de karşılamak için doğmuştur. Her bir alanda çeşitli faaliyetleri gerçekleştirirken de kağıt ortamından mikrofiş, ses bandı, video bant, manyetik bant, manyetik disk, ve optik diske kadar çok çeşitli kayıt ortamlarını da kullanmaktadır (Özdemirci,1996, s. 8).

Elektronik Belge ; klavye, tarayıcı, kamera, video, müzik seti, elektronik posta, teleks, faks vb. araçlar aracılığıyla bilgisayar ortamına aktarılan her çeşit metin, ses, görüntü ve grafik bilgilerinden oluşan belge şeklinde tanımlanabilir (Ödabaş,1999, s. 359)

Elektronik belge yönetimi; kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinden kurum aktivitelerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format, ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetmektir (Kandur, 2005, s. 2).

Elektronik Belge Yönetimi

Dünyada ve ülkemizde son yıllarda büyük değişimler yaşanmış, gelişen, değişen teknoloji ve beraberinde getirdiği uygulamalar yaşamın tüm alanlarında etkili olmuş ve büyük yenilikler getirmiştir. Bu gelişmeler, belge kavramına da elektronik belge kavramı gibi kavramlar eklemiş, kurumlarda elektronik belge, elektronik belge yönetimi önem kazanmıştır. Elektronik belge, elektronik belge yönetimi kavramları; belge, belge yönetimi kavramlarıyla aynı içeriğe sahiptir. Temel farkı bu tür belgelerin elektronik ortamda kullanılıyor olmasıdır. Bu kavramların günlük hayata girmesinde kuşkusuz en büyük faktör dünyadaki teknolojik gelişmeye bağlı olarak ortaya çıkan e-uygulamalardır. Bu tarz e-uygulamalar ülkemizde de e-Türkiye, e-Devlet gibi başlıklar altında planlanmış ve uygulamaya konulmuştur.

Elektronik belge yönetimi bilgi teknolojilerindeki gelişmelere paralel olarak ortaya çıkan ve bu gelişme oranında kurumsal yapıya yansıyan bir

belge yönetim aktivitesidir. Özellikle bilgisayar teknolojisiyle birlikte kurumlar artık belgelerini bilgisayar ortamında üretmekte ve aynı sistem içinde iletimini yapmaktadır. Elektronik belgeler genel olarak bir bilgisayar sistemi bünyesinde üretilen, işlenen ve saklanan belgeleri tanımlar. Elektronik belge yönetimi de bu tür belgelerin yönetilmesini ifade eder. Elektronik belgelerin yönetiminde oluşabilecek olumsuzluklar, yöneticilerin doğru bilgilerle karar almalarında işlevsel devamlılık ve sorumluluk açısından kayıtta birtakım olumsuzlukların oluşması sonucunu doğuracaktır. Bu tip sorunlar kötü bir şekilde yönetilmiş kağıt belge yönetim sistemlerinde olmakta ancak bu elektronik belgelerde daha hızlı ve ani gerçekleşmektedir. Elektronik belgeler, kağıt belgelerde olduğu gibi üretiminden imhasına kadar iyi bir yönetim gerektirir. Elektronik belge yönetimi prensipleri kağıt belgelerin yönetiminden farklı değildir; kaydedilmeye, belirli bir formda tutulmaya, kağıt belgede olduğu gibi ulaşılabilir olmasına gerek vardır. Açıkçası belgeyi bulunduğu ortamda yönetmek tek başına elektronik belge yönetimine yardımcı olamaz. Bununla birlikte elektronik belgeleri üretildiği anda yönetmeye başlamak gereklidir. Aslında denetim elektronik belgeler üretilmeden önce başlanmalıdır. Sistemin tasarım aşamasında her bir belgenin üretimi ve tanımlamalar ile ilgili sistematik bir şekilde saklama süreleri ve imha tarihleri belirlenmeli, güvenli ulaşım ve rahat koruma, belli belgeleri kullanma ve güncellemeyle ilgili konularda yetkilendirmeler yapılmalıdır. Bu nitelemelerin birçoğu rutin belge yönetim aktiviteleridir ve kağıt belgeler için belgenin sonraki yaşam döngüsünde de alınabilir. Ancak elektronik belgelerin üretilmesine başlamadan önce, e-belge yönetim sistemi oluşturulmalıdır (Aydın, 2005, s.92).

Elektronik Belge Yönetim Sistemleri

- Dokümanların üzerinde değişiklik yapılmasına izin verir ya da dokümanların sistem içerisinde birden fazla versiyonu bulunabilir.
- Belgelerin değiştirilmesine izin vermez.
- Belgelerin üreticileri tarafından imha edilmesine izin verebilir.
- Belgelerin imha edilmesine kesinlikle izin vermez. Belgeler ancak saklama planları çerçevesinde kontrollü ortamlarda imha edilebilir.
- Kesinlikle saklama planları içermelidir.
- Belgelerin depolanmasının kontrolü üreticileri tarafından sağlanır.
- Belge yöneticisi ve sistem yöneticisi tarafından tanımlanmış tasnif sistemine bağlı depolama işlemleri gerçekleştirilir.
- Temelde kurumun günlük işlerini daha etkin ve hızlı bir şekilde yapmasına yöneliktir.

➢ Günlük işlerin yapılmasının yanı sıra kurumsal hafızanın korunması ve kurumsal faaliyetlere delil teşkil eden belgelerin güvenilirliğinin sağlanmasına yöneliktir (Kandur, 2005, ss. 2-3).

Günümüzde, vatandaşların devletle ilişkilerindeki ihtiyaçları ve beklentilerin esas olarak değişmesi devlet tanımında da göze çarpar bir şekilde farklılaşmalara neden olmuştur. Daha iyi bir kamu hizmeti için, vatandaşların ihtiyaçlarına göre devletten vatandaşlara, doğrudan bilgi akışını içeren yeni bir yönetim şeklinin tanımlanmasına gereksinim doğmuştur. Ülkemizde, karşılaşılan aksaklıkların düzeltilmesi amacıyla, kamu yönetimlerinin yeniden yapılandırılması faaliyetleri sürmektedir. Bu faaliyetlerde amaç; genelde, ülke yönetiminde çağdaş yapısal değişimleri gerçekleştirmek, özelde, yönetimi bilgi teknolojisi üzerine uyarlamaktır. Bilgi çağının getirdiği değişim; vatandaşı, kendisine hizmet sağlayanlara daha da yakınlaştırarak, kendi ihtiyaçları doğrultusunda daha aktif hale getirmiştir. Bu yaklaşımda, yürütme organı olarak e-Hükümet, temelde vatandaşın ihtiyaçlarına daha iyi hizmet vermekle ilgilenmektedir. e-Hükümet, yürütmenin teknik politikalarını ve kamu sektörünün birbirine uygun bilgi sistemlerinin bir temel çatı altında beraber çalışabilirliğini saptamaktadır. e-Hükümet, bilgiye erişime ve vatandaşa hizmet sunumunu geliştirmeye yardım edecek yorumları ve yenilikleri toplayarak uygulamaya almaktadır (Banger, 2001, s. 5).

Elektronik belge de, e-Devlet çalışmaları kapsamında hem kurum içi çalışmalarda ve iletişimde hem de vatandaşla olan ilişkilerde kullanılan elektronik ortamlarda verilen hizmet kapsamında yerini almıştır. Yerini almasıyla beraber bazı sorunları da beraberinde getirmiştir. Bu sorunlardan biri de elektronik ortamda iletilen belgelerin imzalanması bir başka deyişle onaylanması, sahiplenilmesi sorunudur. Bu sorunların çözümüne yönelik yukarıda açıkladığımız gibi elektronik imza, sayısal imza gibi yöntemler geliştirilmiştir. Bu yöntemlerin hukuki boyutta geçerliliğinin sağlanması ve yaygınlaşması için gerekli yasal düzenlemeler yapılmış ve ilgili kanunlar çıkarılmıştır. Elektronik belgelerde, elektronik veya sayısal imzanın kullanılması ve toplumda yaygınlaştırılması yolunda devlet öncü rol üstlenmeli, bu amaçla kamuda tür uygulamaları yürürlüğe sokmalı, hatta pilot bölge uygulamaları oluşturulmalıdır.

Kurumlarda ise, bu uygulamaların detaylı bir planlaması yapılmalı, hangi birimlerde, kimlerin, hangi durumlarda, ne gibi sınırlandırmalar kapsamında yetkilendirileceğinin organizasyonu çok iyi yapılmalı ve çalışanlara bu kapsamlar içerisinde sorumluluklar verilmelidir.

Bu konudaki en önemli noktalardan biri de elektronik belgelerin saklanmasıdır. Bu amaçla kurum içinde mutlaka bilgi yönetim birimleri bulunmalı bilgi uzmanları istihdam edilmelidir. Bilgi uzmanları ise elektronik belgelerin

saklanması, gerektiğinde hizmete sunulması vb. tüm faaliyetleri, klasik hizmet anlayışını elektronik ortama uyarlayarak yürütmelidir. Tabii ki elektronik ortamda hizmet sunmak bazı farklılıklar doğuracaktır. Ama temelde hizmet anlayışı birbirine paraleldir. Mühim olan, bilgi uzmanlarının kendilerini teknolojik yeniliklere ayak uyduracak şekilde eğitip, geliştirebilmeleri; aynı şekilde de kurumlardaki yönetimin de, hem belge yönetiminde hem de elektronik belge yönetiminde belge yönetim birimlerinin ve bilgi uzmanlarının ne denli önemli bir yere sahip olduklarını algılayarak bu konudaki hassas yaklaşımları sergileyebilmeleridir.

Bilgi teknolojileri, son on yılda çok hızlı gelişme göstermiş ve büyük çaplı bilgisayar ağları, elektronik belgelerin kopyalarının uzak bir mekâna hızlı bir şekilde iletme imkanı tanımıştır. Böylece kağıt kopyalara olan ihtiyaç belli oranda ortadan kalkmaktadır. İnternet'teki web sayfaları, kurumsal politika ve işlevlerin dinamik bir şekilde ve kopyalarını saklamaya ihtiyaç duymadan kullanıcıların ulaşmasına imkan tanımaktadır. Belgeleri kağıt kullanmadan üretip saklama, imha etme ve belge merkezine bir kopyasını gönderme özelliklerine sahip elektronik belge yönetim programları bilgi teknolojilerindeki gelişmelerle birlikte ortaya çıkmıştır. Artık kurumların işlevleri gereği üretilen belgelerin, iletim ve saklanması daha etkin bir biçimde bilgisayar sistemleri aracılığıyla yerine getirilmektedir. Bilgisayarda kelime işlemci uygulamalarıyla yazışmaları üretmek, kalem, kağıt veya daktiloyla üretmekten daha verimli olmaktadır; bu bağlamda elektronik belge yönetimi üzerinde durulması ve beraberinde karşılaşılan sorunların, bir belge yönetim aktivitesi olarak çözülmesi gereği ortaya çıkmaktadır. Çağımızın bu yeni ürününü etkin bir şekilde yönetmek kurumsal başarı açısından çok önemlidir (Aydın, 2005, s. 96).

Kaynakça

Elektronik İmza Kanunu: Kanun no: 5070 (23.01.2004). *T.C. Resmi Gazete* (25355), 1-7.

Ahi, M.G. (2003). *Hukuki bakımdan (dijital) sayısal imza.* 19 Nisan 2006 tarihinde http://www.hukukcu.com/bilimsel/kitaplar/sayisalimza.htm adresinden erişildi.

Anbar, A. (2004). Veri transferi ve işlem güvenliğinin sağlanmasında kullanılan şifreleme yöntemleri ve sayısal imza. *İş, Güç Endüstri ve İnsan Kaynakları Dergisi*, 6 (2). 14 Mart 2006 tarihinde http://www.isgucdergi.org/index.php?arc=arc_view.php&ex=223&inc=arc&cilt=6&sayi=2&year=2004 adresinden erişildi.

Aydın, C. (2005). Bilgi teknolojilerinin belge yönetimine etkisi ve elektronik belge yönetimi. *Bilgi Dünyası,* 6, 89-97.

Banger, G. (2001). *e-Türkiye*. 11 Mart 2006 tarihinde T.C: Başbakanlık İdareyi Geliştirme Başkanlığı web sitesinden erişildi: http://www.edevlet.net/raporveyayinlar/e-turkiye.pdf

Berber, L.K. (2001). *Şekil ve dijital imza*. 20 Mart 2006 tarihinde http://www.hesy.de/sekil/SEKIL_VE_DIJITAL_IMZA.htm adresinden erişildi.

Beydoğan, A. (2005). Elektronik sertifika pazarı ve rekabet. *Telekom Dünyası*, (Şubat), 42-44. 21 Mart 2006 tarihinde http://www.telekomdunyasi.com/OLD/arsiv/2005/Subat2005/aid17.htm adresinden erişildi.

Bilgi, belge ve açıklamaların elektronik ortamda imzalanarak gönderilmesine ilişkin uygulama esasları. 11 Mart 2006 tarihinde Sermaye Piyasası Kurulu Kamuyu Aydınlatma Platformu web sitesinden erişildi: http://www.spk.gov.tr/kap/kurul_kararlari/eisis_ilke_karari.pdf

Civelek, S.P. (2004). *Elektronik imza dönemi başladı: Mevzuat e-imzaya ilişkin neler getiriyor.* 5 Mart 2006 tarihinde http://www.turkhukuksitesi.com/makale_208.htm adresinden erişildi

Demirel, İ. (2006). *Çeşitli ülkelerde uygulanan elektronik ticaret ve elektronik imza yasaları hakkında not.* 16 Mart 2006 tarihinde http://bilisimsurasi.org.tr/dosyalar/7.doc adresinden erişildi.

Digital signature guidelines tutorial. 19 Mart 2006 tarihinde American Bar Association web sitesinden erişildi: http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

Doğan, V. (2005). *Dijital veri güvenilirliği.* 11 Mart 2006 tarihinde Dokuz Eylül Üniversitesi http://courses.cs.deu.edu.tr/cse428/assignment1/VolkanDogan_digital%20signature.doc adresinden erişildi.

Elektronik İmza. (2004). 23 Mart 2006 tarihinde Telekomünikasyon Kurumu web sitesinden erişildi: http://www.tk.gov.tr/eimza/E-Imza_Faydali_bilgiler.htm

Elektronik Ticaret Koordinasyon Kurulu [ETKK]. (1998). *Hukuk Çalışma Grubu Raporu.* 8 Ekim 2005 tarihinde http://www.e-ticaret.gov.tr/raporlar/hukuk.htm adresinden erişildi.

Freeman, E.H. (2004). Digital signatures and electronic contracts. *Information Systems Security,* 13, 8-12.

Gerwig, K. (2000). Business: the 8th layer: will the digital signature transform e-commerce? *netWorker,*4 (3):13-16.

Gupta, A.,Tung,Y.A. ve Marsden, J.R. (2004). Digital signature: Use and modification to achieve success in next generational e-business processes. *Information & Management,* 41, 561-575.

Kandur, H. (2005). Elektronik belge yönetimi sistem kriterleri referans model (v.1.0). 20 Mart 2006 tarihinde Devlet Arşivleri Genel Müdürlüğü web sitesinden erişildi: http://www.devletarsivleri.gov.tr/EBYS_v_1_0.pdf

Kırçova, İ. (2003). *e-Devlet uygulamaları ve ekonomiye etkileri.* İstanbul: İstanbul Ticaret Odası.

Kuechler, W. ve Grupe, F.H. (2002). Digital signatures: A business view. *Information Systems Security,* 11, 23-36.

Mason, S. (2005). Digital signatures: is that really you [electronic signatures]. *IEE Engineering Management,* 15, 10-13.

Moore, M.M. (2001). What is a digital signature? *Darvin*, (Ağustos).17 Mart 2006 tarihinde http://www.darwinmag.com/learn/curve/column.html?ArticleID=144 adresinden erişildi.

Odabaş, H. (1999). Elektronik belgeler ve arşivler. Özlem Bayram…ve başkaları (Yay. Haz.). *Bilginin serüveni: dünü, bugünü ve yarını…Türk Kütüphaneciler Derneği'nin Kuruluşunun 50. Yılı Uluslararası Sempozyum Bildirileri 17-21 Kasım 1999, Ankara* içinde (ss. 356-365). Ankara:Türk Kütüphaneciler Derneği.

Odabaş, H. (2003). Kurumsal bilgi yönetimi. *Türk Kütüphaneciliği,* 17, 357-368.

Özdemirci, F. (1996). *Kurum ve kuruluşlarda belge üretiminin denetlenmesi ve belge yönetimi.* İstanbul: Türk Kütüphaneciler Derneği İstanbul Şubesi.

Özdemirci, F. (2004). Bir disiplin olarak belge yönetimi. Sacit Arslantekin ve Fahrettin Özdemirci (Haz.). *Kütüphaneciliğin Destanı Uluslararası Sempozyumu 21-24 Ekim 2004, Ankara: (Bildiriler) = The Saga of Librarianship International Symposium 21-24 October 2004, Ankara: (Proceedings)* içinde (ss. 191-210). Ankara: A.Ü. DTCF Bilgi ve Belge Yönetimi Bölümü.

Özyılmaz, A. ve Evsenel, S. (2000). Elektronik imza. *Active Dergisi*, (14). 22 Aralık 2005 tarihinde http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=397 adresinden erişildi.

Samast, Y. (2005). *Elektronik imza (e-imza) ve Türkiye*. 11 Mart 2006 tarihinde http://www.muhasebetr.com/e_imza/04.asp adresinden erişildi.

Sayısal imza. 21 Aralık 2005 tarihinde http://www.turkpoint.com/e-yasa/sayisal_imza.asp adresinden erişildi.

Srivastava, A. (2005). Is Internet security a major issue with respect to the slow acceptance rate of digital signatures. *Computer Law & Security Report,* 21, 392-404.

Tansal, Ş. (2005). Elektronik imza yasası. *Elektrik Mühendisliği* (425 Şubat), 90-93. 18 Mart 2006 tarihinde Elektrik Mühendisleri Odası web sitesinden erişildi: http://www.emo.org.tr/resimler/ekler/4f683a84163b352_ek.pdf adresinden erişildi.

Tansuğ, A. (Şubat 2002). *Dijital imza ve yasal düzenleme yaklaşımları: Bilişim Şurası Hukuk Çalışma Grubu Raporu.* 15 Mart 2006 tarihinde Bilişim Şurası web sitesinden erişildi: http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0000/01-TBS_DIJITAL_IMZA_TANSUGdoc.doc

Tüfekçi, T. (t.y.). Elektronik imza için neredeyiz. 18 Aralık 2005 tarihinde http://www.tubitak.gov.tr adresinden erişildi.

Tüfekçi, T. (2002). *Elektronik imza niçin yaygınlaşamıyor*. 21 Mart 2006 tarihinde Türkiye Bilişim Derneği web sitesinden erişildi: http://kurultay.tbd.org.tr/kurultay20/Bildiriler/Tolga_Tufekci/bildiri.pdf

Zaba, S. (2006). Digital signature legislation: The first 10 years. *Information Security Technical Report, 11*, 18-25.